TELKOMNIKA Telecommunication, Computing, Electronics and Control
Vol. 18, No. 4, August 2020, pp. 2004~2011
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v18i4.14748

QR code based authentication method for IoT applications using three security layers

Abbas M. Al-Ghaili[1], Hairoladenan Kasim[2], Marini Othman[3], Wahidah Hashim[4]
[1,3,4]Institute of Informatics and Computing in Energy, Universiti Tenaga Nasional, Malaysia
[2]College of Computing & Informatics, Universiti Tenaga Nasional, Malaysia

Article Info

Article history:

Received Aug 1, 2019
Revised Jan 11, 2020
Accepted Apr 13, 2020

Keywords:

Data authentication
Data security
Internet of Things
QR code

ABSTRACT

A quick response code-based authentication method (QRAM) is proposed. QRAM is applicable for lots of internet of things (IoT) applications. QRAM aims to verify requests of such an access to IoT applications. Requests are made using a quick response code (QRC). To authenticate contents of QRC, users will scan QRC to access IoT applications. To authenticate contents of QRC, three procedures are applied. QRAM contributes to IoT automatic access systems or smart applications in terms of authentication and safety of access. QRAM is evaluated in term of security factors (e.g., authentication). Computation time of authentication procedures for several IoT applications has become a considerable issue. QRAM aims to reduce computation time consumed to authenticate each QRC. Some authentication techniques still face difficulties when an IoT application requires fast response to users; therefore, QRAM aims to enhance so to meet real-time applications. Thus, QRAM is compared to several competitive methods used to verify QRC in term of computation time. Results confirmed that QRAM is faster than other competitive techniques. Besides, results have shown a high level of complexity in term of decryption time needed to deduce private contents of QRC. QRAM also is robust against unauthorized requests of access.

Corresponding Author:

Abbas M. Al-Ghaili,
Institute of Informatics and Computing in Energy (IICE),
Universiti Tenaga Nasional (UNITEN),
43000 Kajang, Selangor, Malaysia.
Email: abbas@uniten.edu.my

1. INTRODUCTION

Nowadays, many researches that deal with the use of quick response (QR) code in security-related services [1] have been reviewed. Some of these examples are included in [2-7]. The technology of quick response code (QRC) has been utilized by many applications [8-13]. The QRC is suitable for data privacy and can be a good tool to protect data [14] using encryption schemes. There are many applications that focus on data authentication in order to verify that data are originally issued and contents have not been changed in an authorized manner.

Authentication is a very important consideration for several applications because it affects the performance of the system in term of security and confidentiality. Many other related security issues could also be affected in such a case authentication has not been securely and efficiently considered. Therefore, the proposed method in this paper aims to verify once an unauthorized modification has occurred or not. It has considered a number of verification procedures due to the information encrypted inside the QRC has to

be always private and confidential. Another reason that a secure authentication method is important for internet-of-things (IoT) application is that, this information inclusive in the QRC is used to access a data-sensitive IoT application. The proposed QR based authentication method (QRAM) in this paper is applied on QRC to verify security objectives.

In literature review, many IoT applications have been proposed some of which have suggested and designed authentication systems and some others have performed evaluation procedures. From these, a number of QRC-based methods have been performing smart services utilizing the QRC itself. But the very important thing to consider is that: are these QRC-based IoT applications authenticated. For example, there exist many systems concern authentication, data privacy, and security such as internet of things (IoT) [15], smart applications [16], cryptography and data encryption [17, 18], data transfer [19], public key encryption scheme [20], and cloud computing resources' authentication [21]. This has contributed to a smart life environment [22] in terms of data privacy, security, and computation time.

In general, these proposed systems may fail to achieve a high level of security. One of the biggest issues is when the application becomes susceptible for unusual actions. However, there exist several attempts to propose secure applications e.g., [23, 24] in which their aims are to protect data and attain authentication. These examples have designed a QRC based authentication mechanism for users in order to prevent threats and to increase security of users' private contents.

The QRC is a very effective technology for many IoT applications in terms of safety and authenticity e.g., these reviewed in [25-28]. Thus, in [21] a QRC technology has been used in order to perform an authentication procedure for users engaged with an cloud computing environment. QRC has a good feature that is it can store a huge portion of information in a very small area. A lot of IoT applications can exploit such a feature and re-use it based on needs [29]. Many examples are in detailed reviewed in [7, 19, 30-40]. Therefore, these contents of QRC can be verified in terms of authentication and privacy. Usually, the verification process concerns contents of QRC. If contents of QRC have not been changed in an unauthorized manner, the privacy of QRC can be considered as attained and QRC is private.

Therefore, related data needs to be private and secure. Additionally, the related applications should be confidential with the help of QRC technique. In order to do so, a strong security scheme needs to be and the verification process of QRC contents has to be precise. Hence, in this paper, the verification procedure with several security layers are considered. So, the verification procedure consists of a number of steps in order to increase the security of contents of QRC. The proposed QRAM is applied on QRC to verify security objectives. In addition, it verifies the authenticity of QRC.

Simply, the QRAM has performed three authentication procedures each of which is applied to a single part of QRC content to produce its distinguished output. Once this procedure has been applied, the computation time is expected to be reduced. For security purposes, the verification procedures will stop immediately and will not go for the next layer's verification if the following possibility has occurred which is: the case that one layer has produced a wrongly compared result. Thus, QRAM instantly halts the verification procedure.

There are however many difficulties and challenges still. Thus, there have been research studies attempting to overcome those challenges. An example of those challenges might be a compensation of a technique to be fast-responsive to real-time IoT applications and robust enough against threats. Thus, in order to meet real-time applications, further enhancement is needed. Therefore, QRAM aims to enhance authentication procedures applied to IoT applications that depend on QRC in terms of computation time.

The organization of this paper is presented as follows: in section 2, the proposed methodology of QRAM is in detail explained. Results and Discussion will be discussed in section 3. Conclusion is drawn in section 4.

2. THE PROPOSED QRAM

Simply, the proposed methodology of QRAM contains three types of authentication verification procedure. The first one is a user frequently-updated image (UI) authentication, the second one is a user activity-derived number (UAN) authentication, and the third authentication is user_ID (UID). They are graphically presented and shown in Figure 1. The flowchart of QRAM is illustrated in Figure 2.

2.1. UI authentication

Each user will be assigned a distinctive QRC in order to be authenticated. In this procedure, the UI will be captured. The QRAM will process it and extract certain information and distinctive values. These values and information will be sent to the QRAM's database in order to perform a real-time comparison. If the UI is identical to its corresponding values which are stored in database. The system will consider that the UI is authenticated and valid. Hence, the QRAM accepts the QRC and moves forward to check other

security factors with UAN and UID. Otherwise, the QRAM rejects the currently processed QRC and stops the whole procedure from being accessed by un-authorized parties.

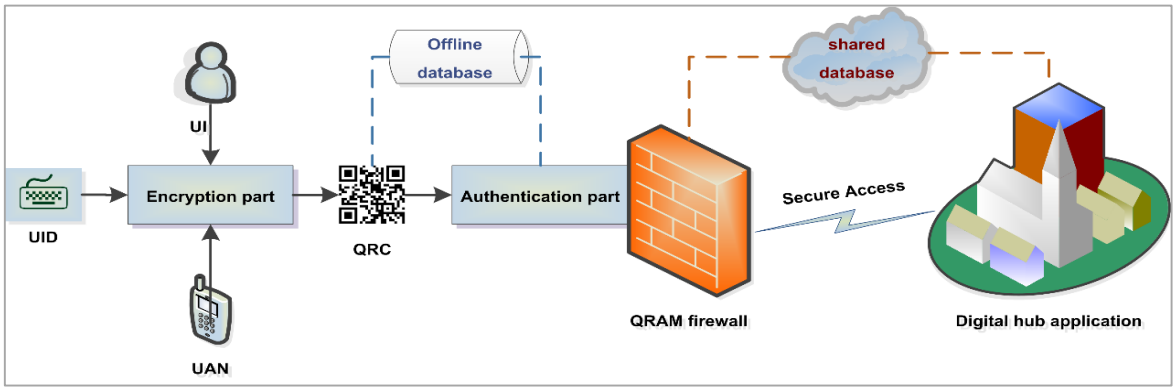

Figure 1. A Graphical Overview of the Proposed QRAM

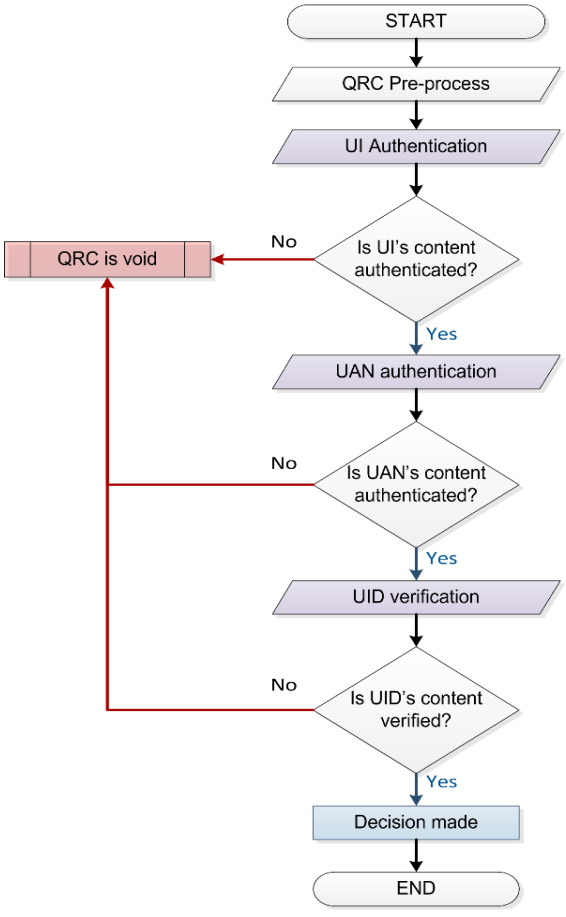

Figure 2. The Proposed QRAM Flowchart

2.2. UAN authentication

UAN contains two steps, which are encryption and verification, as shown in Figure 3. The proposed QRAM determines certain values to be encrypted first. Usually, values which are determined for encryption process are selected based on latest activities done by the user. Then, these values are mathematically re-produced using a pseudorandom number generator (PRNG). Then, they will be formalized as a mathematically ordered

numbers queued in an array. This array will be encrypted to produce an un-known number called user activity-derived number (UAN). The whole above-mentioned process inclusive the encryption scheme is performed periodically. Every time, the QRC is generated, the new UAN is included in order to make sure that the QRC is always updated and contains new input values e.g., UAN.

UAN is verified by the QRAM to make sure that UAN is created using recently active values. If the UAN has been encrypted using recent values, that means the QRC is new and surely is different from the currently used one. That is because the UAN is one of the QRC's inputs. Thus, the database is updated and the authentication process compares its new values to QRC values once the user is required by the system to send requests.

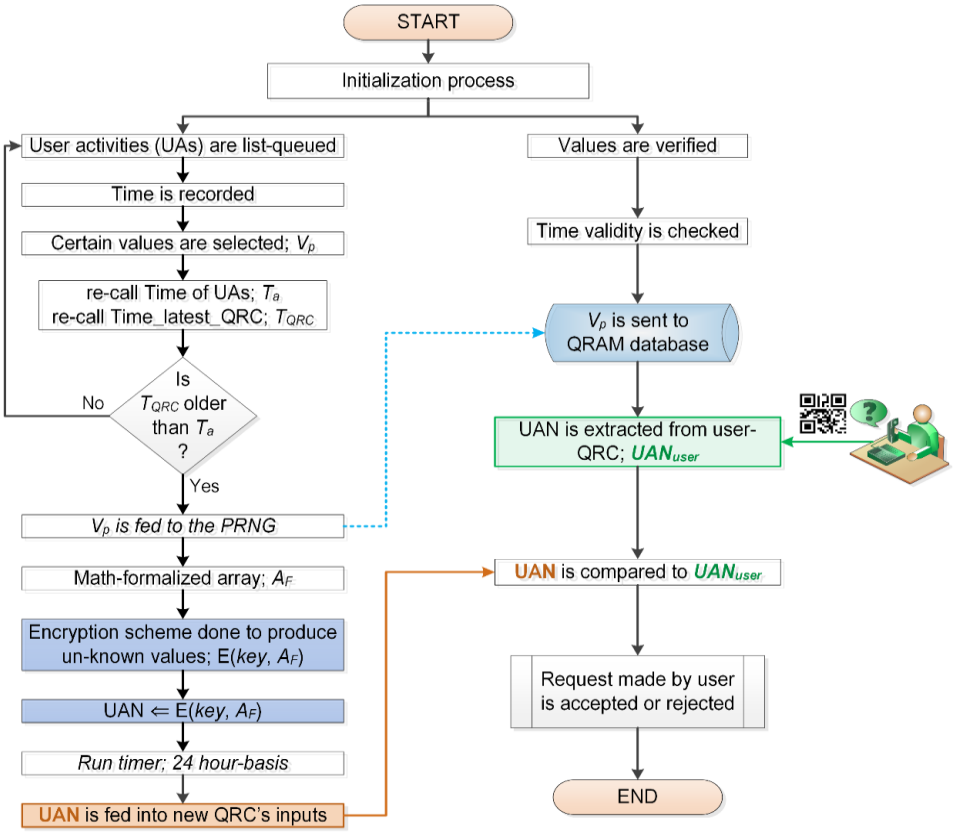

Figure 3. The UAN Flowchart (encryption left-hand side and verification right-hand side)

2.3. UID authentication

In this procedure, there will be a *lookup table* designed to store all encrypted information such as UAN, E (key, A_F), T_a, and T_{QRC}. These values are recalled once an access has been made by the user and when the QRC is scanned. The UID verification will be carried out using this table. Selected values will be chosen to perform a comparison between UID stored in this table to UID encrypted inside the QRC. This is discussed as follows:

Each user is assigned a distinctive UID that was previously produced. This UID is stored in the offline database. To make sure whether the user has entered the correct UID or not, a mathematical procedure is applied. The following steps can add more clarification, explained as follows:

- Two neighboring users *UIDs* located as a predecessor and successor with index-values as: $user\_id(i-1)$ and $user\_id(i+1)$, respectively, are selected; marked in Figure 4.
- Extract binary values (UID_{b-1}, and UID_{b+1}) for $UID(i-1)$ and $UID(i+1)$, respectively, by applying (1) and (2):

$$UID_{b-1} = binary(UID(i-1)) \quad (1)$$

$$UID_{b+1} = binary(UID(i+1)) \quad (2)$$

- Apply (3) and (4) to normalize binary values to a certain length of digits:

$$id\_1_{normalized} = Norm(UID_{b-1}) \quad (3)$$

$$id\_2_{normalized} = Norm(UID_{b+1}) \quad (4)$$

when the UID_{b-1} being normalized, the value will be compared to all values stored in lookup table in order to guarantee there will be no similarity between any two digital numbers. Meaning each id_i will be distinctive from all *i*th values for any UID_ith value; thus: $\forall i \in \{id\_i \mid 0 \leq i \leq users_{max}\}$.
where,

- $id_$i represents the UID number for the user (i),
- $\text{users}_{\max}$ is the number of users registered in database.

The following inequation becomes true to store related values in the lookup table for authentication purposes.

$$id\_(i-2) \neq id\_(i-1) \neq id\_(i) \neq id\_(i+1) \neq id\_(i+2) \neq \cdots \neq id\_(i)th$$

This is to produce a distinctive hash value in the next step.

- Apply (5) on these two index-values to obtain hash values:

$$ID\_i_{hashed} = Hash(id\_1_{normalized} \oplus id\_2_{normalized} \oplus M) \quad (5)$$

UID	**value**
i-3	0
i-2	1
i-1	2
i	3
i+1	4
i+2	5
i+3	6

► value (***UID(i)***) =3

Figure 4. UID(i) and its Neighboring UIDs' table

3. RESULTS AND DISCUSSION

In this section, the performance of the proposed QRAM will be anlaysed. The obtained results after the QRAM has been applied will be discussed and evaluated. The QRAM will be evaluated in term of authentication and computation time.

3.1. Authentication

The QRC contents are verified and authenticated. Usually contents of QRC stored in database will be compared to QRC owned by the user. The content of UAN-based verification will be considered. This procedure takes into account the following considerations while the QRC is authenticated, which are as follows:

- Time of issue of QRC; T_{QRC}
- Time of user activities recordings; T_a
- $UAN_{database}$ is compared to UAN stored inside the user's QRC, UAN_{user};
- Encrypted values will be decrypted;

The pseudo-code of the UAN-based authentication is shown in Algorithm 2 to add more explanation of security factor analysis; i.e., authentication.
Algorithm 1: UAN authentication pseudo-code as a verification tool

```
set variables as T=0, QRC=False;
call following functions: f(T_QRC), f(T_a), f (E (key, AF);
decrypt QRC owned by the user; //QRC_user
decrypt QRC stored inside database; //QRC_database
extract UAN_user
extract UAN_database
If (UAN_user==UAN_database) {// to ensure if QRC is old
             If (T_QRC<T_a)
                          If (Timer==True) {
```

```
                                        T=1;
                                        QRC=True;}
                          Else
                          T=0;
               Else
               QRC is true but QRC is old and no more is used;}
Else
               QRC is expired;
End If
If (T==1)
               message="Request is Accepted";
Else
               message="Request is Rejected";
End If
```

Algorithm 1 ensures that there is no modification on contents of QRC in terms of its date of issue. Therefore, it adds an if-statement based condition: if (Timer==True). If this condition is true, then T=1 and authentication is accepted in terms of validity and expiry date. That surely means the QRC is successfully updated.

3.2. Computation time

QRAM in term of computation time is evaluated. The computation time needed to perform one operation (i.e., inclusive UI, UAN, and UID authentication) on a single QRC is considered. Simply, related computation time(s) are calculated using C++ *time* functions. The obtained computation time is compared to several competitive techniques as shown in Table 1.

As noticeable in Table 1, the computation time of QRAM is less than certificate and [23]'s methods. The blue color fields show the techniques have used in comparison. The green color fields show how many QR codes have been used in experiment, i.e., samples size. The yellow color fields show the computation time consumed for each technique per every sample size. The red color fields show the averaged computation time for all techniques. It is obviously clear that the proposed QRAM comes in the 2nd rank amongst other techniques with an averged computation time equals to 293.64 mS with 1.696 times faster than the certificate technique. For a more clarification, performance evaluation of the proposed QRAM is provided in which it is compared to other competitive techniques as shown in Figure 5. As shown in Figure 5, the proposed QRAM's computation time is located in the second rank.

Table 1. QRAM computation time compared to other techniques; time in millisecond (mS)

Technique	**Number of QR codes used in experiments**					
	10	50	100	150	300	
	Computation time in mS					**Averaged computation time**
Password	24.9	115.6	205.1	346.7	622.2	262.9
[23]	31.4	149.0	313.3	444.5	807.8	349.2
Certificate	45.2	212.6	452.2	637.1	1143.9	498.2
Proposed QRAM	**28.6**	**132.1**	**226.7**	**390.6**	**690.2**	**293.64**

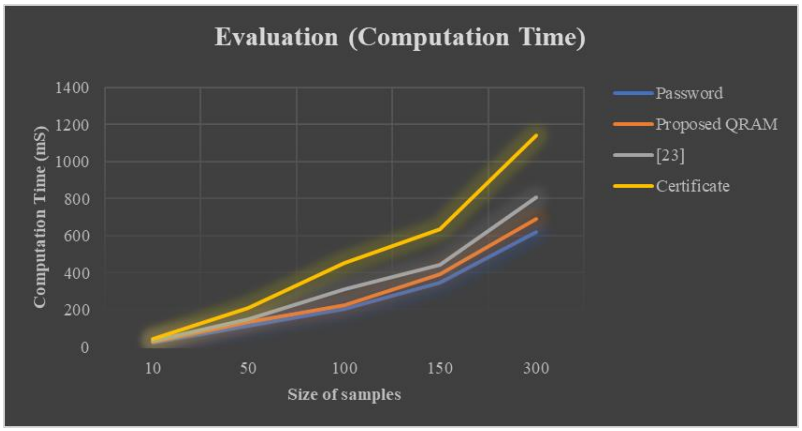

Figure 5. Performance evaluation in terms of computation time

3.3. Robustness based on key length against brute force attack

Length of secret key is evaluated. The QRAM has adopted two different key-lengths with sizes of 320 and 384 bits. This evaluation supposes that when the QRAM has used a key of length equals to 320 and 384 bits, the decryption time of brute force attack-based scheme needs about 3.4×10^{76} and 6.3×10^{95} years, respectively. Thus, QRAM is robust.

4. CONCLUSION

This paper has proposed a simple verification method utilizing QRC to authenticate its contents. QRAM purpose is to apply several steps applied on several layers to increase security of contents of an IoT application. There will be three verification procedures implemented to do so which are: UI, UAN, and UID. This proposed mechanism also aims to reduce the computation time. QRAM by then makes a decision either to accept or reject such a request of an access to the related IoT application. A request of an access is made using a QRC and therefore the QRAM securely authenticates contents of QRC. Results confirmed that the QRAM is faster than other competitive techniques. In addition, results have shown a high level of complexity in terms of decryption time needed to deduce the QRC's secret key. Obtained results confirmed that the QRAM is robust against unusual threats and potential actions. The QRAM is important to work with applications which require online verification processes. Future works are dedicated to enhance computation time to work in a faster environment under complex scenarios e.g., when there are more than two parties requiring a response in a same time.

ACKNOWLEDGEMENT

This research is funded by Universiti Tenaga Nasional (UNITEN) with grant code: (BOLD2025-10436494/B/2019115)

REFERENCES

[1] R. Focardi, F. L. Luccio, and H. A. M. Wahsheh, "Usable security for QR code," *Journal of Information Security and Applications*, vol. 48, p. 102369, 1 October 2019.
[2] Y. Wang, C. Sun, P. Kuan, C. Lu, and H. Wang, "Secured graphic QR code with infrared watermark," in *2018 IEEE International Conference on Applied System Invention (ICASI)*, pp. 690-693, 2018.
[3] Y. Cheng, Z. Fu, and B. Yu, "Improved Visual Secret Sharing Scheme for QR Code Applications," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2393-2403, 2018.
[4] Z. Fu, Y. Cheng, and B. Yu, "Visual Cryptography Scheme With Meaningful Shares Based on QR Codes," *IEEE Access*, vol. 6, pp. 59567-59574, 2018.
[5] J. Song, K. Gao, X. Shen, X. Qi, R. Liu, and K.-K. R. Choo, "QRFence: A flexible and scalable QR link security detection framework for Android devices," *Future Generation Computer Systems*, vol. 88, pp. 663-674, 2018.
[6] Y. Qin, Z. Wang, H. Wang, and Q. Gong, "Binary image encryption in a joint transform correlator scheme by aid of run-length encoding and QR code," *Optics & Laser Technology*, vol. 103, pp. 93-98, 2018.
[7] Y. Wei, A. Yan, J. Dong, Z. Hu, and J. Zhang, "Optical image encryption using QR code and multilevel fingerprints in gyrator transform domains," *Optics Communications*, vol. 403, pp. 62-67, 2017.
[8] P. Nazemzadeh, D. Fontanelli, D. Macii, and L. Palopoli, "Indoor Localization of Mobile Robots Through QR Code Detection and Dead Reckoning Data Fusion," *IEEE/ASME Transactions on Mechatronics*, vol. 22, no. 6, pp. 2588-2599, 2017.
[9] S. Demir, R. Kaynak, and K. A. Demir, "Usage Level and Future Intent of Use of Quick Response (QR) Codes for Mobile Marketing among College Students in Turkey," *Procedia - Social and Behavioral Sciences*, vol. 181, pp. 405-413, 2015.
[10] M. K. Schultz, "A case study on the appropriateness of using quick response (QR) codes in libraries and museums," Library & Information Science Research, vol. 35, no. 3, pp. 207-215, 2013.
[11] S. Goyal, S. Yadav, and M. Mathuria, "Exploring concept of QR code and its benefits in digital education system," in *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 1141-1147, 2016.
[12] A. M. Al-Ghaili, H. Kasim, F. A. Rahim, Z. A. Ibrahim, M. Othman, and Z. Hassan, "Smart verification algorithm for IoT applications using QR tag," *Lecture Notes in Electrical Engineering*, vol. 481, pp. 107-116, 2019.
[13] A. M. Al-Ghaili, H. Kasim, M. Othman, and Z. Hassan, "Security Factors Based Evaluation of Verification Algorithm for an IoT Access System," in *International Conference of Reliable Information and Communication Technology*, 2018: Springer, pp. 384-395, 2018.
[14] T. Kirkham, D. Armstrong, K. Djemame, and M. Jiang, "Risk driven Smart Home resource management using cloud services," *Future Generation Computer Systems*, vol. 38, pp. 13-22, 2014.
[15] A. Čolaković and M. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," *Computer Networks*, vol. 144, pp. 17-39, 2018.

[16] S. Rane, A. Dubey, and T. Parida, "Design of IoT based intelligent parking system using image processing algorithms," in *2017 International Conference on Computing Methodologies and Communication (ICCMC)*, pp. 1049-1053, 2017.
[17] A. Paverd et al., "OmniShare: Encrypted Cloud Storage for the Multi-Device Era," *IEEE Internet Computing*, vol. 22, no. 4, pp. 27-36, 2018.
[18] A. M. Al-Ghaili, H. Kasim, M. Othman, and Z. Hassan, "A New Encryption Scheme Method (ESM) Using Capsulated-Layers Conception for Verified QR-Tag for IoT-Based Smart Access Systems," in Internet of Things and Big Data Analytics for Smart Generation, V. E. Balas, V. K. Solanki, R. Kumar, and M. Khari Eds. Cham*: Springer International Publishing*, pp. 77-103, 2019.
[19] N. V. Akhil, A. Vijay, and D. S. Kumar, "QR code security using proxy re-encryption," in *2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT)*, pp. 1-5, 2016.
[20] S. Sun, S. Han, D. Gu, and S. Liu, "Public key cryptosystems secure against memory leakage attacks," *IET Information Security*, vol. 10, no. 6, pp. 403-412, 2016.
[21] D.-S. Oh, B.-H. Kim, and J.-K. Lee, "A Study on Authentication System Using QR Code for Mobile Cloud Computing Environment," Berlin, Heidelberg, 2011: *Springer Berlin Heidelberg*, in Future Information Technology, pp. 500-507, 2011.
[22] S. S. I. Samuel, "A review of connectivity challenges in IoT-smart home," in *2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC)*, pp. 1-4, 2016.
[23] Y. G. Kim and M. S. Jun, "A design of user authentication system using QR code identifying method," in *2011 6th International Conference on Computer Sciences and Convergence Information Technology (ICCIT)*, pp. 31-35, 2011.
[24] G. Jaspher, W. Katherine, E. Kirubakaran, and P. Prakash, "Smart card based remote user authentication schemes: Survey," in *Computing Communication & Networking Technologies (ICCCNT), Third International Conference on 2012*, pp. 1-5, 2012.
[25] J. Su et al., "i-Logistics: An intelligent Logistics system based on Internet of things," in *2017 International Conference on Applied System Innovation (ICASI)*, pp. 331-334, 2017.
[26] L. Russell, R. Goubran, and F. Kwamena, "Sensing instrumentation using smartphones: Securing impact and awareness," in *2018 IEEE International Instrumentation and Measurement Technology Conference (I2MTC)*, pp. 1-5, 2018.
[27] M. Togan, B. Chifor, I. Florea, and G. Gugulea, "A smart-phone based privacy-preserving security framework for IoT devices," in *2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, pp. 1-7, 2017.
[28] M. Suresh, P. S. Kumar, and T. V. P. Sundararajan, "IoT Based Airport Parking System," in *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, pp. 1-5, 2015.
[29] A. M. Al-Ghaili, F. A. Rahim, F. Azman, and H. Kasim, "Efficient Implementation of 2D Barcode Verification Algorithm for IoT Applications," in *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, pp. 282-287, 27-29 May 2019.
[30] C. Yao, "Constructing a User-Friendly and Smart Ubiquitous Personalized Learning Environment by Using a Context-Aware Mechanism," *IEEE Transactions on Learning Technologies*, vol. 10, no. 1, pp. 104-114, 2017.
[31] M. Edinger, D. Bar-Shalom, N. Sandler, J. Rantanen, and N. Genina, "QR encoded smart oral dosage forms by inkjet printing," *International Journal of Pharmaceutics*, vol. 536, no. 1, pp. 138-145, 2018.
[32] P.-C. Huang, C.-C. Chang, Y.-H. Li, and Y. Liu, "Efficient access control system based on aesthetic QR code," *Personal Ubiquitous Comput.*, vol. 22, no. 1, pp. 81-91, 2018.
[33] T. Kobayashi, R. Nakashima, R. Uchida, and K. Arai, "SNS Door Phone as Robotic Process Automation," *presented at the Proceedings of the 2018 ACM International Conference on Interactive Surfaces and Spaces*, Tokyo, Japan, 2018.
[34] Y. Zhou et al., "Method of multiple-image hiding in QR code based on compressed sensing and orthogonal modulation," *Optik*, vol. 159, pp. 265-274, 2018.
[35] J. Qian, X. Du, B. Zhang, B. Fan, and X. Yang, "Optimization of QR code readability in movement state using response surface methodology for implementing continuous chain traceability," *Computers and Electronics in Agriculture*, vol. 139, pp. 56-64, 2017.
[36] D. Rosario-Raymundo and M. Rowena, "QR codes as mobile learning tools for labor room nurses at the San Pablo Colleges Medical Center," *Interactive Technology and Smart Education*, vol. 14, no. 2, pp. 138-158, 2017.
[37] C. Liu et al., "DNA Barcode Goes Two-Dimensions: DNA QR Code Web Server," PLOS ONE, vol. 7, no. 5, p. e35146, 2012, doi: 10.1371/journal.pone.0035146.
[38] T. M. Fernandez-Caramés and P. Fraga-Lamas, "A Review on Human-Centered IoT-Connected Smart Labels for the Industry 4.0," *IEEE Access*, vol. 6, pp. 25939-25957, 2018.
[39] S. Tiwari, "An Introduction to QR Code Technology," in *2016 International Conference on Information Technology (ICIT)*, pp. 39-44, 2016.
[40] N. Taveerad and S. Vongpradhip, "Development of Color QR Code for Increasing Capacity," in *2015 11th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)*, pp. 645-648, 2015.